



New OCR Guidance for Phase II HIPAA Audits

H. Carol Saul and Madison M. Pool

HHS Office for Civil Rights (OCR) recently issued guidance addressing its approach to the 2016 Phase II HIPAA Desk Audits.¹ In its announcement of the guidance, OCR emphasized the broader applicability of these resources beyond just the 167 covered entities currently selected for Phase II Desk Audits, saying, “[t]he guidance should be helpful to audited entities as well as other covered entities and business associates seeking assistance with improving their compliance with these important requirements of the HIPAA Rules.”² The insight provided in these documents may be especially useful to business associates in anticipation of the Business Associate Desk Audits which OCR has said will commence in late September of this year.³

OCR provided this new guidance in three documents:

- Selected Protocol Elements with associated document submission requests and related Q&As (“Protocol”);
- Slides from audited entity webinar held July 13, 2016 (“Presentation”); and
- Comprehensive question and answer listing (“Q&A”).

Protocol

The Protocol includes sections for Audit Inquiry, Document Request List, and related Questions/Answers (excerpted from the Q&A document). The Audit Inquiries were excerpted from the general Phase 2 HIPAA Audit Program Audit Protocol, updated in April 2016⁴; this further emphasizes the importance for covered entities and business associates of reviewing OCR guidance as it is issued and incorporating it into their ongoing compliance efforts.

The Document Request List gives additional insight into the kinds of documentation OCR considers necessary for compliance with the selected regulatory sections. Some items of particular note:

- In the inquiry regarding Notices of Privacy Practices provided electronically, OCR requests to see “documentation of an agreement with the individual to receive the notice via e-mail or other electronic form.”⁵ Although the cited regulation requires that an individual must agree to receive the Notice of Privacy Practices electronically, there is not an express requirement for the form that agreement must take. Thus, the request for “*an agreement with the individual*” underscores OCR’s emphasis on documentation.

¹ See <http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html> (last accessed Aug. 1, 2016); see also AGG Client Alert, OCR Update: HIPAA Phase 2 Audit Notices—Responses Due July 22, 2016 (July 14, 2016), <http://www.agg.com/OCR-Update-HIPAA-Phase-2-Audit-NoticesResponses-Due-July-22-2016-07-13-2016> (last accessed Aug. 3, 2016).

² Posting of OCRPrivacyList@HHS.GOV to OCR-PRIVACY-LIST@LIST.NIH.GOV, *Updates to the HHS Office for Civil Rights Webpages: HIPAA Audit Guidance & FAQ on HIPAA and Unique Device Identifiers* (July 27, 2016, 7:37 a.m.) (on file with author).

³ HHS-OCR, HIPAA Privacy, Security & Breach Notification Compliance Audits Phase 2, Informational Webinar, slide 10, available at <http://www.hhs.gov/sites/default/files/OCRDeskAuditOpeningMeetingWebinar.pdf> [hereinafter Presentation] (last accessed Aug. 1, 2016).

⁴ HHS-OCR, Audit Protocol – Updated April 2016, available at <http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html> (last accessed Aug. 1, 2016).

⁵ HHS-OCR, OCR 2016 HIPAA Desk Audit Guidance on Selected Protocol Elements, available at <http://www.hhs.gov/sites/default/files/2016HIPAADeskAuditAuditeeGuidance.pdf> [hereinafter Protocol] (last accessed Aug. 1, 2016).

- Throughout the communications regarding the Phase II Audits, OCR has emphasized compliance with the Security Rule. In relation to the Security Management Process, the Protocol requests “documentation demonstrating the efforts used to manage risks from the previous calendar year,” and “documentation demonstrating the security measures implemented to reduce risks as a result of the current risk analysis or assessment. (Upload documentation demonstrating that current and ongoing risks [are] reviewed and updated.)”⁶ These requests highlight that OCR views risk assessment and management not as a one-time exercise, but rather as a continual, dynamic process responsive to changes in real time.

Presentation

Some points of interest from the Presentation include that OCR anticipates that onsite audits will begin in early 2017, and may include both covered entities that were subject to the Desk Audits, as well as newly selected covered entities not previously part of the Desk Audit process.⁷ Notification of these onsite audits is expected in late fall.⁸ OCR also noted in the Presentation that the onsite audits will evaluate auditees against a comprehensive set of HIPAA compliance controls, suggesting that onsite audits may not be limited in scope in the same way as the Desk Audits.⁹

Q&A

The Q&A document primarily contains questions and answers directly related to the Desk Audit process itself, while also providing helpful insight to business associates in anticipation of the upcoming Business Associate Desk Audits. The document also offers a more general understanding of what OCR considers appropriate documentation to support requests. For example, in response to the question “Do[es OCR] wish to receive pictures of the Notices [of Privacy Practices] hanging on the walls in addition to receiving the uploaded paper copies?” OCR responded, “Yes. Please ensure the text is readable.”¹⁰ Another example of the specificity and detail OCR is expecting in supporting documentation comes in answer to the question, “[Audit Item] P65 Right to Access - If the access request is from a personal representative on behalf of the patient, are we required to submit documentation proving the personal representative’s authority?” OCR responded, “P65 requires all documentation related to the specified access requests. That would include documentation of personal representative status when such status is relevant to the handling of the request.”¹¹

Conclusion

OCR’s newly released guidance documents, as well as the full 2016 Audit Protocol and other guidance available on OCR’s website, are important tools for covered entities and business associates to use in reviewing and strengthening their compliance with HIPAA. Although OCR has indicated that the Phase II Audits are a “compliance tool,”¹² multiple recent high-dollar settlements and Resolution Agreements—with covered entities and business associates alike—give an indication of the direction OCR is trending regarding enforcement of HIPAA compliance.

⁶ *Id.*

⁷ Presentation at slide 8.

⁸ HHS-OCR, OCR 2016 HIPAA Desk Audits – Audited Entity Questions and Answers, *available at* <http://www.hhs.gov/sites/default/files/Phase2AuditOpeningMeetingWebinarQ%26A.pdf> [hereinafter Q&A] (last accessed Aug. 1, 2016).

⁹ Presentation at slide 8. Note that the Desk Audits were limited to seven specific areas of review (see Presentation at slide 13).

¹⁰ Q&A #43.

¹¹ *Id.* #48

¹² Q&A #27.

Authors and Contributors

H. Carol Saul

Partner, Atlanta Office
404.873.8694
carol.saul@agg.com

Madison M. Pool

Associate, Atlanta Office
404.873.8514
madison.pool@agg.com

not *if*, but *how*.[®]

About Arnall Golden Gregory LLP

Arnall Golden Gregory, a law firm with more than 150 attorneys in Atlanta and Washington, DC, employs a “business sensibility” approach, developing a deep understanding of each client’s industry and situation in order to find a customized, cost-sensitive solution, and then continuing to help them stay one step ahead. Selected for The National Law Journal’s prestigious 2013 Midsize Hot List, the firm offers corporate, litigation and regulatory services for numerous industries, including healthcare, life sciences, global logistics and transportation, real estate, food distribution, financial services, franchising, consumer products and services, information services, energy and manufacturing. AGG subscribes to the belief “not if, but how.” Visit www.agg.com.

Atlanta Office

171 17th Street, NW
Suite 2100
Atlanta, GA 30363

Washington, DC Office

1775 Pennsylvania Avenue, NW
Suite 1000
Washington, DC 20006

To subscribe to future alerts, insights and newsletters: <http://www.agg.com/subscribe/>

©2016. Arnall Golden Gregory LLP. This legal insight provides a general summary of recent legal developments. It is not intended to be, and should not be relied upon as, legal advice. Under professional rules, this communication may be considered advertising material.